

## Notice of Allowability

Application No.

09/651,619

Examiner

Aravind K. Moorthy

Applicant(s)

BOIVE, RICHARD H.

Art Unit

2131

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 4/24/2007.
2. ☒ The allowed claim(s) is/are 1-23.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All b) ☐ Some\* c) ☐ None of the:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

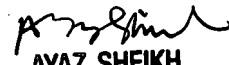
4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
    - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
    - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

### Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),  
Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit  
of Biological Material

5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413),  
Paper No./Mail Date \_\_\_\_\_
7. ☒ Examiner's Amendment/Comment

8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

  
**AYAZ SHEIKH**  
**SUPERVISORY PATENT EXAMINER**  
**TECHNOLOGY CENTER 2100**

### **DETAILED ACTION**

1. This is in response to the arguments filed on 24 April 2007.
2. Claims 1-23 are pending in the application.
3. Claims 1-23 have been allowed.

#### ***Response to Arguments***

4. Applicant's arguments, see pages 9-13, filed 24 April 2007, with respect to claims 1-23 have been fully considered and are persuasive. The rejection of the claims has been withdrawn.

#### ***Allowable Subject Matter***

5. Claims 1-23 are allowed.

The following is an examiner's statement of reasons for allowance:

The current application is directed towards a backtracking method, program and unit that involves a traceback computer program for tracking a denial-of-service attack on a victim machine, v, back toward the source of the denial-of service attack. The traceback program determines a set of routers that are upstream neighbors of v and determines which of those neighbors is the principal source of packets flowing to v. After determining the identity of the neighbor node, n, that is the principal source of packets flowing to v, the traceback program continues further upstream from n to determine the upstream neighbor of n that is the principal source of packets to v. After determining this upstream neighbor, the program continues further upstream until the source of the denial-of-service packets is determined.

The closest prior art to the current application was Stone et al U.S. Patent No. 7,062,782 B1 (hereafter Stone). Stone is directed towards an approach for tracking denial-of-service (DoS) flood attacks using an overlay IP (Internet Protocol) network. One or more tracking routers form

Art Unit: 2131

an overlay tracking network over the network of an Internet Service Provider (ISP). The ISP network includes numerous transit routers and edge routers. The tracking routers communicate directly with all the edge routers using IP tunnels. The edge routers within the ISP network perform security diagnostic functions, in part, to identify a DoS flood attack that has been launched by one or more attackers. To track down an attacker, an egress edge router identifies the DoS flood attack datagrams, rerouting these datagrams to the overlay tracking network. The tracking routers perform hop-by-hop input debugging to identify the ingress edge router associated with the source of the DoS flood attack.

However, there are differences between Stone and the current application. Stone lacks the following step recited in independent method claim 1: "if r is n's next hop for traffic addressed to v, determining an amount of traffic that n is forwarding to r that is addressed to v". Stone does not teach the step as follows: "based on the determined amounts of traffic of said neighbors, determining the identity of the neighbor n of r that is the principal source of packets flowing to r that are addressed to v; continuing one node further upstream from the determined neighbor n of r that is the principal source of packets flowing to r that are addressed to v". Independent apparatus claim 9 recites similar steps. Stone merely discusses the scaling of an overlay network to accommodate larger numbers of edge routers. Stone's scaling activity has nothing to do with a determination "an amount of traffic that n is forwarding to r that is addressed to v" as recited in independent claims 1 and 9. Stone also lacks the above quoted step of determining the identity of a neighbor n or r that is the principal source of packets flowing to r that are addressed to v. Stone merely describes a computer system 801 that can perform trace back activities, but does not describe the above quoted step of independent claims 1 and 9.

Art Unit: 2131

Independent method claim 22 is similar to independent method claim 1 to recite: "determining a count of packets that router n is sending to router r that are addressed to v or to a network on which v resides; based on the determined counts of packets of said neighbors n, determining the identity of the neighbor n of r that is the principal source of packets flowing to r that are addressed to v". Stone does not disclose the feature of determining the amount of traffic or the step of determining the neighbor n or r that is the principal source of packets flowing to r that are addressed to v. Therefore, Stone also lacks the above quoted portions of independent method claim 22. With respect to independent method claim 16, Stone lacks the following step: "querying individual ones of packet routers in order to determine a packet router that is a largest source of packets addressed to v via r, or to a network to which v is connected, and continuing to query packet routers up through a hierarchy of interconnected packet routers until an identity of a source of the undesirable packets is discovered or until further backtracking is not possible". Stone does not disclose or teach "order to determine a packet router that is a largest source of packets addressed to v via r". Moreover, Applicant's method and system achieves traceback without the expense of an extra overlay network and extra tracing routers that Stone uses.

Any claims not directly addressed are allowed on their virtue of dependency.


Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

***Conclusion***

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy   
July 2, 2007

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100